Pearson BTEC Level 3 Nationals Diploma, Extended Diploma

Window for supervised period:
Tuesday 10 January 2023 to Monday 30 January 2023

Supervised hours 4 hours

Paper reference **20158K**

Information Technology

UNIT 11: Cyber Security and Incident Management

Part B

You must have:
Forensic_Analysis.rtf

Instructions

- **Part A** and **Part B** contain material for the completion of the set tasks under supervised conditions.
- There are 43 marks for **Part A** and 37 marks for **Part B**, giving a total mark for the set tasks of 80.
- **Part A** and **Part B** are specific to each series and this material must be issued only to learners who have been entered to take the tasks in the specified series.
- This booklet should be kept securely until the start of the 4-hour, **Part B** supervised assessment period.
- **Part A** will need to have been completed and kept securely before starting **Part B**.
- Both parts will need to be completed during the 3-week period timetabled by Pearson.
- **Part A** and **Part B** tasks must be submitted together for each learner.
- **Part A** materials must not be accessed during the completion of **Part B**.
- This booklet should not be returned to Pearson.
- Answer **all** activities.

Information

- The total mark for this Part is 37.

Turn over ▶

Pearson

Instructions to Invigilators

This paper must be read in conjunction with the unit information in the specification and the *BTEC Nationals Instructions for Conducting External Assessments (ICEA)* document. See the Pearson website for details.

Refer carefully to the instructions in this task booklet and the *BTEC Nationals Instructions for Conducting External Assessments (ICEA)* document to ensure that the assessment is supervised correctly.

Part A and **Part B** set tasks should be completed during the period of 3 weeks timetabled by Pearson. **Part A** must be completed before starting **Part B**.

The 4-hour **Part B** set task must be carried out under supervised conditions.

The set task can be undertaken in more than one supervised session.

An electronic template for activity 4 is available on the website for centres to download for learner use.

Learners must complete this task on a computer using the templates provided and appropriate software. All work must be saved as PDF documents for submission.

Invigilators may clarify the wording that appears in this task but cannot provide any guidance in completion of the task.

Invigilators should note that they are responsible for maintaining security and for reporting issues to Pearson.

Maintaining Security

- Learners must not bring anything into the supervised environment or take anything out.
- Centres are responsible for putting in place appropriate checks to ensure that only permitted material is introduced into the supervised environment.
- Internet access is not permitted.
- Learner's work must be regularly backed up. Learners should save their work to their folder using the naming instructions indicated in each activity.
- During any permitted break, and at the end of the session, materials must be kept securely and no items removed from the supervised environment.
- Learners can only access their work under supervision.
- User areas must only be accessible to the individual learners and to named members of staff.
- Any materials being used by learners must be collected in at the end of each session, stored securely and handed back at the beginning of the next session.
- Following completion of **Part B** of the set task, all materials must be retained securely for submission to Pearson.
- **Part A** materials must not be accessed during the completion of **Part B**.

Outcomes for Submission

Each learner must create a folder to submit their work. Each folder should be named according to this naming convention:

[Centre #]_[Registration number #]_[surname]_[first letter of first name]_U11B

Example: Joshua Smith with registration number F180542 at centre 12345 would have a folder titled

12345_F180542_Smith_J_U11B

Each learner will need to submit 2 PDF documents, within their folder, using the file names listed.

Activity 4: activity4_incidentanalysis_[Registration number #]_[surname]_[first letter of first name]

Activity 5: activity5_securityreport_[Registration number #]_[surname]_[first letter of first name]

An authentication sheet must be completed by each learner and submitted with the final outcomes.

The work should be submitted no later than 1 February 2023.

Instructions for Learners

Read the set task brief carefully.

Plan your time carefully to allow for the preparation and completion of all the activities.

Your centre will advise you of the timing for the supervised period. It is likely that you will be given more than one timetabled session to complete these tasks.

Internet access is not allowed.

You will complete this set task under supervision and your work will be kept securely at all times.

You must work independently throughout the supervised assessment period and must not share your work with other learners.

Your invigilator may clarify the wording that appears in this task but cannot provide any guidance in completion of the task.

Part A materials must not be accessed during the completion of **Part B**.

Outcomes for Submission

You must create a folder to submit your work. The folder should be named according to the following naming convention:

[Centre #]_[Registration number #]_[surname]_[first letter of first name]_U11B

Example: Joshua Smith with registration number F180542 at centre 12345 would have a folder titled

12345_F180542_Smith_J_U11B

You will need to submit 2 PDF documents, within your folder, using the file names listed.

Activity 4: activity4_incidentanalysis_[Registration number #]_[surname]_[first letter of first name]

Activity 5: activity5_securityreport_[Registration number #]_[surname]_[first letter of first name]

You must complete an authentication sheet before you hand your work in to your invigilator.

Set Task Brief

Guiding Lighting

Paul Jones is the owner of Guiding Lighting (GL). The business makes and maintains lighting systems for emergency routes such as fire exits. The lighting systems include illuminated information panels and lights built into floors and walls to indicate the route that people should use to find the nearest exit in an emergency.

Paul is developing a new product that makes use of Internet of Things (IoT) technology. He has installed a pilot system at the Heritage Crafts Open Air Museum. The museum exhibits crafts and occupations from several historical periods.

The devices in the IoT network will connect to each other using the Zigbee protocol. Zigbee is a low-power WiFi protocol that incorporates mesh networking and uses IPv6 addresses.

Visitors download an app onto a mobile device and select the exhibits that they wish to visit. The app then calculates the best route and GL's smart lighting will guide them from place to place. The app will connect to the IoT network using WiFi or Bluetooth.

Client brief

You advised Paul on cyber security matters for a prototype system at GL's headquarters. Now, a few weeks later, Paul has asked you to review the investigation of a recent cyber security incident at the museum.

The incident involved an intermittent problem that occurred over the weekend, starting on the 6th January.

Visitors started to complain that the guiding lighting had stopped working for them. They were able to select exhibits to visit and the system started them on a route. Then at various points around the route the system seemed to lose contact with them. The lights no longer gave correct directions, or just stopped working.

Usually the visitors were able to reconnect after a short time but had to restart the app.

Evidence items from the security incident at the Heritage Crafts Open Air Museum

Evidence items include:

1. Paul's account
2. IT technician's report
3. Incident log
4. Network diagram
5. Map of the museum
6. Cyber security document – incident management policy.

1. Paul's account

It started on Friday 6th January, about 3 p.m. I was at home when I got a phone call from Danika Nowack, one of our technicians. She was on-call for the weekend and had spent the morning trying to fix a problem at the museum.

She knew that I had been involved with the set up of the system and thought I might be able to help. The place is only a few miles away, I got there by 4 p.m. and went straight to the visitor centre where we had a temporary control room for the system **(see evidence item 5)**.

The problem had started shortly after the museum opened at 10 a.m. The guide system was breaking down, seemingly at random. It was still doing that when I got there. In fact it was recovering from a failure as I parked my car at the visitor centre.

The system is designed so that it resets if error signals are received by the control computer, in this case a laptop in the visitor centre **(see evidence item 4)**. The reset process appeared to be working correctly and the guide system functioned as it should after each reset. Each error and reset is automatically reported to GL's headquarters. Danika was called out straight away as this is a pilot system and we want to get all the bugs ironed out before we start selling it commercially.

Danika had already checked the hardware and software. We looked at some other ideas like damaged wiring and water getting into things – it had rained the previous night – but couldn't find anything. The random failures continued until about an hour before closing time at 6 p.m. We packed up shortly afterwards.

The next day was no better and by midday we concluded that there was nothing wrong with the system and that it might be a deliberate attack. We decided to shut the system down and launch an investigation into possible external causes.

2. IT technician's report

Date: 08/01/2023

Written by: Danika Nowack
SIRT leader for incident affecting Guiding Lighting pilot system: GL-IN210701-P

Introduction

This report covers:
- diagnostics of a malfunctioning system at the Heritage Crafts Open Air Museum
- the post-incident discussion of a possible attack on the system.

Diagnostics, factors covered:

(a) Hardware.
External items, information screens and lighting tracks were examined and no signs of tampering were found.
The nearest panel and lighting strip were switched off and replaced temporarily with new items, the guide system remained stable for about an hour and then reset again. The temporary items were removed and the originals switched back on again.
All items except the nearest panel and lighting strip were then switched off. The system reset after about 90 minutes.
Internal items, the IoT router and antennae were swapped with spares at the same time as the nearest panel and lighting strip were replaced.
There were no spares on site for the laptop and 3G router. These were changed first thing on Sunday. This did not stop the guide system from resetting.

(b) Software.
The software in the routers, panels and guide strips are held in firmware. The hash codes were checked and found to be correct.

The laptop software appeared to be running correctly. The software on the second laptop uses the same base program but was set up independently rather than copying the site parameters from the first laptop.
The laptops only contain a minimal Linux OS and the Guiding Lighting control and diagnostics software.

(c) Communications.
All communications to the panels and guide strips are encrypted. Passwords for the system were changed on the Sunday morning but this did not solve the problem.
WiFi and Bluetooth signal strengths were measured at several locations around the museum and all were found to be within the design limits.

(d) Environmental.
The panels and guide strips are sealed units and are unlikely to have been affected by the environment in the short time they have been deployed. They are solar powered with built-in photoelectric cells, so there should not be a problem with, e.g. animals damaging a power supply. Battery levels for the panels and guide strips were checked and found to be within the design limits.
No water damage was found.

There was a concern that vehicles from the exhibitors might have damaged a guide strip but nothing was found.

Post-incident discussion of a possible attack.

Date: 10/01/2023

No further resets happened during the next two days. The incident was closed and the team met to discuss what may have happened.

The CSIRT consisted of:
Danika Nowack, Team Leader
Paul Jones, owner of GL
Brian Smith, Technical Manager for the Heritage Crafts Open Air Museum.

The team concluded that the system had suffered what appeared to be a denial of service attack, but were unable to decide if it was malicious or accidental. We thought of three ways in which the attack could have happened.

1. The Zigbee mesh WiFi or the Bluetooth signals were jammed or spoofed by an outside source. It was not a continuous source as the communications diagnostics had not picked it up.

2. Someone had cracked the GL communications password and was deliberately crashing the system.

3. Some other device or system being operated in or near the museum was leaking radio waves, which interfered with the Zigbee mesh WiFi and/or the Bluetooth signals.

Brian was asked to join the team as he had been involved with setting up the pilot system and is familiar with the technology being used in the museum.

He offered some possible signal sources.

a) Mains electricity cables run under or near several of the GL devices. If one were badly shielded it could generate interference.

b) There were radio controlled camera drones operating on the weekend of the incident, making a publicity film for the museum. The control signals may have interfered.

c) The Edwardian fairground included an electric carousel that was scheduled to offer rides to the public every 30 minutes. The set up included a lorry mounted generator and a lot of electric cables. This could give the same problem as described in (a).

d) A member of the public may have been using a device, deliberately or otherwise, that gave off radio signals.

Paul thought that:

- a password crack could be ruled out due to Sunday's actions
- the drone signal was unlikely to be strong enough, but since Zigbee and Bluetooth use low power WiFi, it was still possible
- a mains cable problem was also unlikely for obvious reasons
- the Edwardian fairground or a device used by a member of the public were the most probable causes.

The team were unable to come to a definitive conclusion. They decided that the incident showed the GL communications system needs to be made more robust to prevent a similar occurrence.

3. Incident log

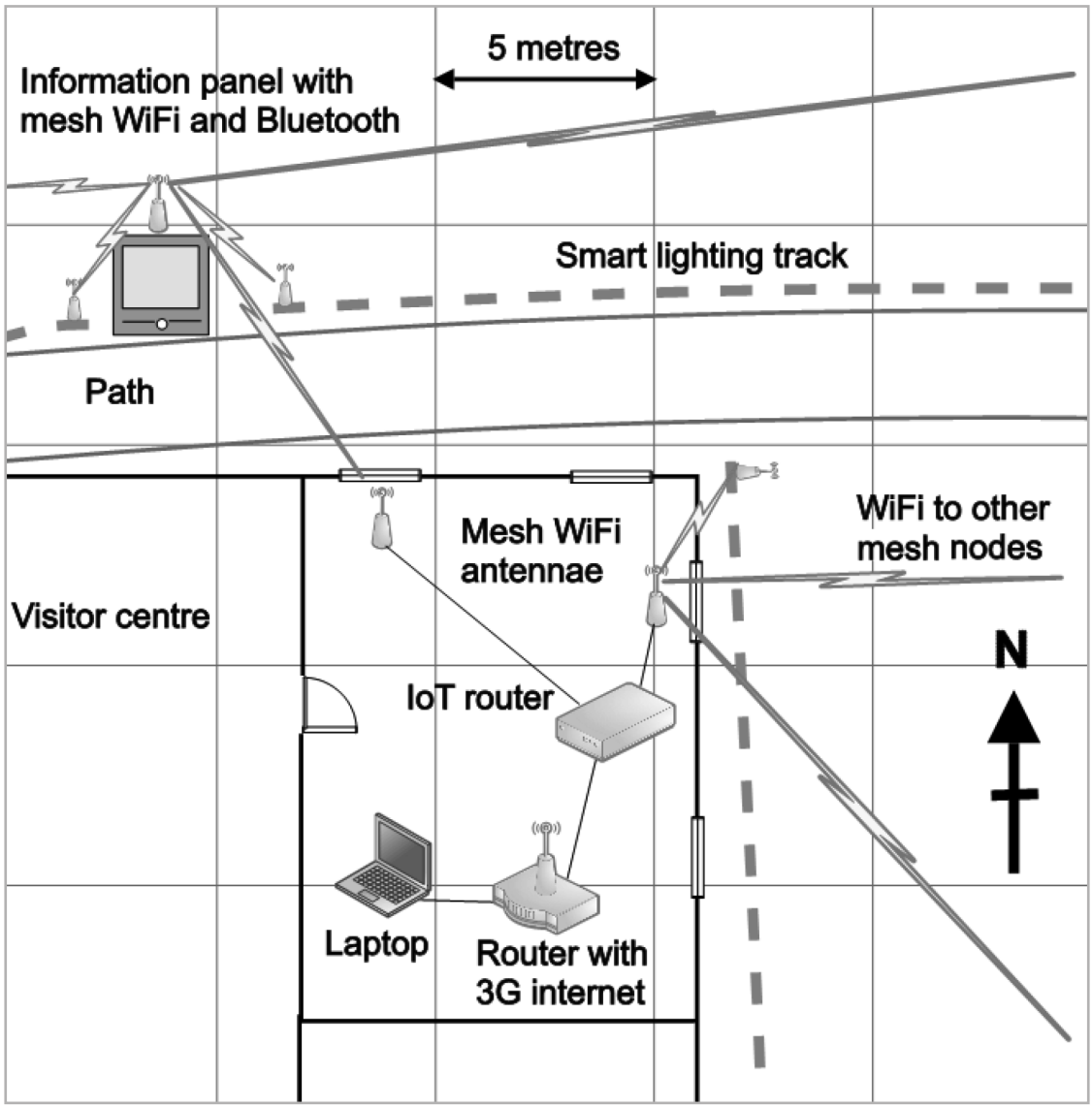
Saturday 7th January

10:25 reset reported by automated system
10:54 reset reported by automated system
10:58 on-call technician, Danika Nowack, asked to attend the pilot system site
11:45 Danika Nowack arrives and starts diagnosing the problem
11:56 system resets
12:00 inspection of hardware, no faults found
12:27 system resets
12:35 temporary replacement of panel and lighting strip
12:45 IoT router and antennae replaced
12:50 diagnostics software used to check firmware and battery levels on routers, panels and guide strips, no problems found
13:26 system resets
13:30 all except nearest panel and guide strip switched off
14:54 system resets
14:56 Paul Jones called out
15:05 check for damage caused by vehicle movements, nothing found
15:35 panels and guide strips switched on again
15:53 system resets
16:04 Paul Jones arrives and is briefed
16:15 check for water leakage at all panels and guide strips, nothing found
16:57 system resets
17:25 system closed down

Sunday 8th January

09:45 laptop and 3G router replaced
09:55 system started
10:05 change passwords
10:15 check signal strengths
10:56 system resets
11:00 reload all firmware on routers, panels and guide strips.
11:27 system resets
11:56 system resets
12:05 system closed down

4. Network diagram



Notes:

The antennae shown on the information panel and smart lighting tracks are built in to the equipment and not accessible to the public.

The antennae on the smart lighting tracks are designed to have a maximum range of five metres and should only link to the nearest information panel or mesh WiFi antenna.

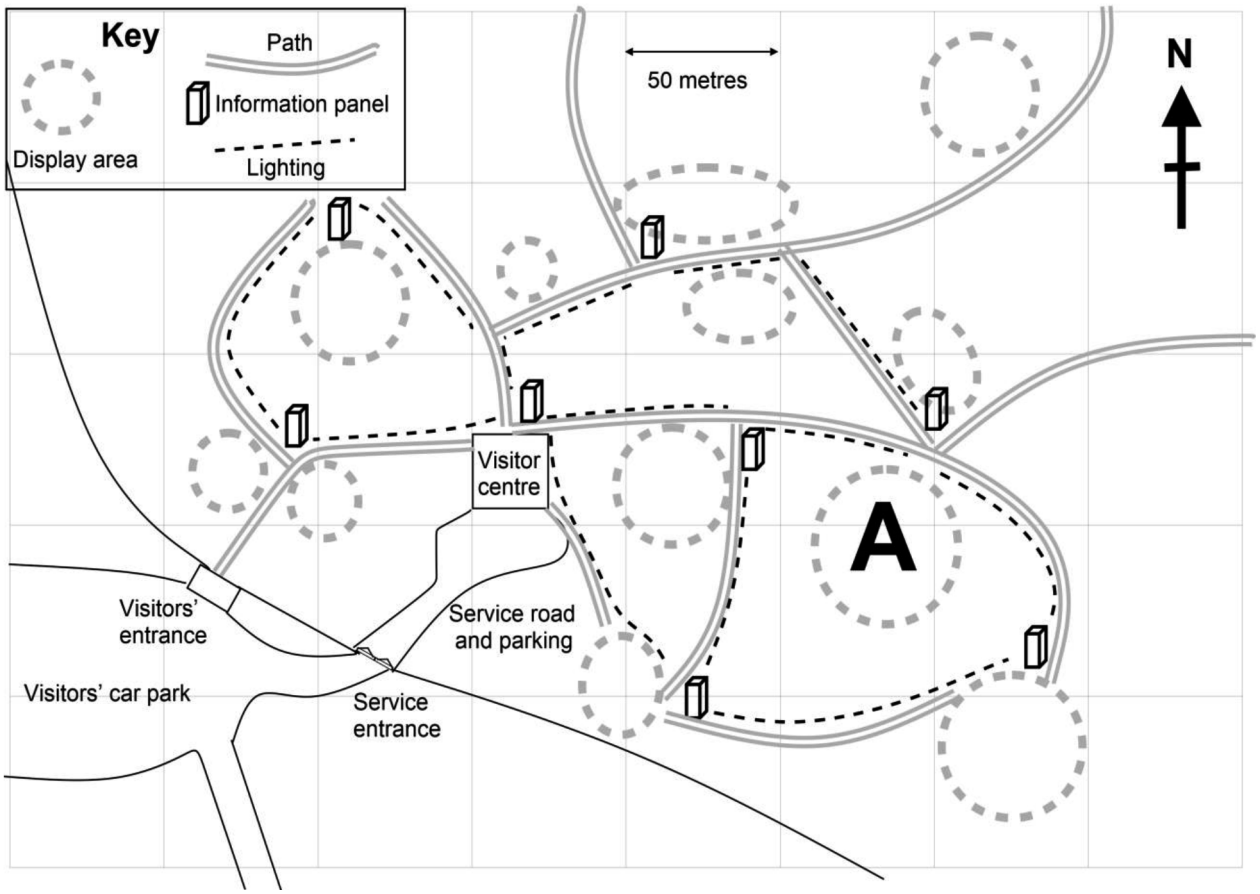
The room used in the visitor centre is in a private section, with no public access. The key is held by the museum when there are no GL personnel on site.

5. Map of the museum

A map of the pilot system at the Heritage Crafts Open Air Museum.

The pilot system only covers those exhibits near to the visitor centre, the rest of the museum is not shown.

On the weekend of the incident some Edwardian fairground rides were exhibited in the area marked **A**. These rides were taken away on the Sunday evening.



6. Cyber security document – incident management policy

Incident management team

The team shall consist of:

- the senior IT technician on site (team leader)
- a representative from the company/organisation hosting the Guiding Lighting system
- personnel co-opted by the team leader as needed.

Incident reporting

Any member of staff who considers that an IT-related security incident has occurred must report it as soon as possible to the Computer Security Incident Response Team (CSIRT) leader.

Initially it may be reported verbally but this must be followed up by an email. It is the responsibility of the CSIRT to maintain detailed documentation on the incident from first report to final resolution.

Security incidents may include:

- theft of IT equipment
- theft of company data
- infection of Guiding Lighting IT systems with malware
- unauthorised access to Guiding Lighting IT systems.

Incident response procedures

(a) Theft of IT equipment

- Theft of IT equipment is a very serious issue. Any thefts must be reported at once to the CSIRT leader, initially a verbal report must be made followed up by email, providing as much information as possible (location and type of equipment, when it was last seen, etc.).
- The CSIRT leader must ascertain if the item has actually been stolen (or if it is just missing).
- If the item is confirmed as stolen, the CSIRT leader must inform the police and contact the finance department so they can inform insurers.
- The CSIRT must prepare a report on the theft for Guiding Lighting management and if needed justify the finances required to replace the stolen item.
- Where personally identifiable data may have been compromised, a separate report must be prepared detailing the possible data breach.

(b) Theft of company data

- Theft or loss of company data may occur in a number of different ways.
- Any loss of company data must be reported at once to the CSIRT leader, initially a verbal report must be made followed up by email.
- The CSIRT must investigate the loss and identify exactly what data has been lost or stolen and when the incident occurred.
- Having identified what has been lost or stolen and when, the CSIRT must retrieve backups and restore the data as soon as possible.
- The CSIRT should review the incident and implement procedures to prevent future losses.
- Where personally identifiable data may have been compromised, a separate report must be prepared detailing the possible data breach.

(c) Infection of IT systems with malware

- Any member of staff who suspects that any IT system has been infected with malware must report at once to the CSIRT leader, initially a verbal report must be made followed up by email.
- The infected system should be shut down as soon as possible.
- The CSIRT will investigate the infection and take appropriate measures to resolve the infection and restore the system.
- Where personally identifiable data may have been compromised, a separate report must be prepared detailing the possible data breach.

(d) Unauthorised access to IT systems

- Any member of staff who suspects that there has been unauthorised access to any Guiding Lighting IT system must report it at once to the CSIRT leader, providing as much detail as possible (which system, how access was obtained). Initially a verbal report must be made, followed up by email.
- The CSIRT will thoroughly investigate the incident and identify how the unauthorised access was obtained.
- The CSIRT will recommend action to prevent future occurrences (e.g. change passwords).
- Where personally identifiable data may have been compromised, a separate report must be prepared detailing the possible data breach.

Part B Set Task

You must complete ALL activities within the set task.

Produce your documents using a computer.

Save your documents in your folder ready for submission using the formats and naming conventions indicated.

Read the set task brief carefully before you begin and note that reading time is included in the overall assessment time.

You have been advising Paul Jones on cyber security. Now he has asked you to review the investigation of a cyber security incident.

Activity 4: Forensic incident analysis

Analyse the forensic evidence, including how the evidence was obtained, for the cyber security incident at the Heritage Crafts Open Air Museum.

Consider possible causes of the incident and come to a conclusion about the most likely cause of the incident.

Refer to evidence items 1–5 inclusive.

Produce a forensic incident analysis using the template **Forensic_Analysis.rtf**

Save your completed forensic incident analysis as a PDF in your folder for submission as **activity4_incidentanalysis_[Registration number #]_[surname]_[first letter of first name]**

You are advised to spend 2 hours on this activity.

(Total for Activity 4 = 14 marks)

Activity 5: Security report

Review the incident. Suggest improvements and explain how they would prevent a similar incident in the future.

Areas for improvement are:

- adherence to forensic procedures
- the forensic procedure and current security protection measures
- the security documentation.

Read the set task brief and evidence items 1–6 inclusive when answering the question.

Save your completed security report as a PDF in your folder for submission as **activity5_securityreport_[Registration number #]_[surname]_[first letter of first name]**

You are advised to spend 2 hours on this activity.

(Total for Activity 5 = 20 marks)

TOTAL FOR TECHNICAL LANGUAGE IN PART B = 3 MARKS
TOTAL FOR PART B = 37 MARKS